UNITED STATES PATENT APPLICATION FOR:

ACCESS CONTROL REPOSITORY FOR PROVIDING ACCESS CONTROL OF SERVICE PROFILES FOR WEB BASED SOLUTIONS

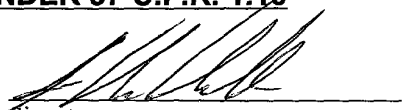
INVENTORS:

SATHEESH K. KRISHNAMOORTHY

ATTORNEY DOCKET NUMBER: ROC920010284US1

CERTIFICATION OF MAILING UNDER 37 C.F.R. 1.10

I hereby certify that this New Application and the documents referred to as enclosed therein are being deposited with the United States Postal Service on December 14, 2001, in an envelope marked as "Express Mail United States Postal Service", Mailing Label No. EL913563906US, addressed to: Assistant Commissioner for Patents, Box PATENT APPLICATION, Washington, D.C. 20231.



Signature

Gero G. McClellan
Name

December 14, 2001
Date of signature

ACCESS CONTROL REPOSITORY FOR PROVIDING ACCESS CONTROL OF SERVICE PROFILES FOR WEB BASED SOLUTIONS

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention generally relates to data processing. More particularly, the invention relates to providing entitlement services data.

Description of the Related Art

[0002] It is well known to couple a plurality of computer systems into a network of computer systems. In this way, the collective resources available within the network may be shared amongst users, thus allowing each connected user to enjoy resources which would not be economically feasible to provide to each user individually. With the growth of the Internet, sharing of computer resources has been brought to a much wider audience. The Internet has become a cultural medium in today's society for both information and entertainment. For many companies, one or more Internet sites are an integral part of their business; these sites are frequently mentioned in the companies' television, radio and print advertising.

[0003] Despite their usefulness, wide area networks such as the Internet present integration problems for many enterprises. Such problems arise, for example, with corporations providing entitlement services to customers. In general, entitlement services include maintenance agreements, service agreements and the like. Such agreements may attach to any of a variety of products offered by the corporation, including hardware and software. In an effort to make this information available to customers corporations typically provide Web based access to entitlement services databases. However, in today's large distributed corporate environment, the entitlement services data as well as the applications providing access thereto tend to be highly diversified. This diversification arises because the business rules underlying the entitlement services vary according to product and geography. In

order to facilitate an expeditious Web based solution for customers, developers focus on a particular entitlement service rather than on a holistic (e.g., global) strategy. As a result, a single customer having made a plurality of purchases in different global regions (e.g., different countries) may be in a position of having to access a multiplicity of web applications in order to access the entitlement services data for each of the products purchased. Even when accessing different entitlement services for the same product (e.g., such as where the customer has entitlement services for a particular type of computer in the United States as well as in the United Kingdom), the user may be required to perform a separate registration step in order to access the entitlement services for each country.

[0004] The foregoing problems may be illustrated with reference to the network environment 100 of FIG. 1. In general, the network environment 100 shows a plurality of client computers 102_1, 102_2...102_N (collectively referred to herein as clients 102) operated by users desiring to access entitlement services databases 114. In a Web-based environment each of the clients 102 execute a browser application 104. During a browser session, a user may ultimately invoke an enterprise application 110_1, 110_2...110_N (collectively referred to herein as applications 110), such as by clicking on a hyperlink. Each application 110 is configured to access a limited number of the entitlement databases 114 via an adapter 112_1, 112_2...112_N (collectively referred to herein as adapters 112).

[0005] Accordingly, no common entitlement system exists. Instead, a plurality of applications 110 were (and continue to be) independently developed to support different products and hence, different entitlement services. Each of the applications 110 define their own entitlement interfaces and provide no connectivity (e.g., data sharing) between one another. The lack of connectivity between applications results in each application having to separately access the entitlement databases 114 for a given customer during a given browser session. In addition, each application is configured to access its own limited number of entitlement databases, resulting in duplication of efforts and resources. Such an environment provides an undesirable interface for customers and substantially complicates development.

[0006] Further, it is often desirable for an enterprise to extend complementary services to its customers. However, where the entitlement services data is distributed over a plurality of databases, no feasible solution for extending such complementary services exists. This is because each application is configured to access only selected databases containing information specific to the services supported by the accessing application. As a result, any given application has no knowledge about entitlement services data contained in another databases serviced by other applications.

[0007] Therefore, there is a need for a method and a system for overcoming the problems associated with existing entitlement services systems.

SUMMARY OF THE INVENTION

[0008] The present invention provides an access control repository for implementing a common entitlement service. The following summaries provide illustrative embodiment and are not intended to define all embodiments within the scope of the invention nor to limit the scope of the invention.

[0009] One embodiment provides a method of providing entitlement services information to users comprising receiving a request for entitlement services information for a particular user; and in response to receiving the request, accessing a common entitlement services information repository. The common entitlement services information repository associates entitlement services with products to which the entitlement services attach and with users of the products. In one embodiment each of at least a portion of the plurality of users is associated with at least two products.

[0010] Another embodiment provides an entitlement services system comprising a common entitlement services information system comprising a repository associating entitlement services with products to which the entitlement services attach and with users of the products; wherein each of at least a portion of the plurality of users is associated with at least two products.

[0011] Still another embodiment provides an entitlement services system, comprising a common entitlement services information system, comprising a repository and an access control software component configured to access the repository in response to entitlement services information requests. The repository associates entitlement services with products to which the entitlement services attach and with users of the products. In one embodiment each of at least a portion of the plurality of users is associated with at least two products. The entitlement services system further comprises at least one server executing a plurality of Web based applications configured to issue the entitlement services information requests and a web server hosting a Web service providing an interface to each of the plurality of applications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] So that the manner in which the above recited features, advantages and objects of the present invention are attained and can be understood in detail, a more particular description of the invention, briefly summarized above, may be had by reference to the embodiments thereof which are illustrated in the appended drawings.

[0013] It is to be noted, however, that the appended drawings illustrate only typical embodiments of this invention and are therefore not to be considered limiting of its scope, for the invention may admit to other equally effective embodiments.

[0014] FIG. 1 is a prior art data processing environment supporting Web based entitlement services.

[0015] FIG. 2 is a high-level diagram of a computer in which aspects of the invention may be implemented.

[0016] FIG. 3 is a distributed environment configured with an access control repository.

[0017] FIG. 4 is a distributed environment configured with an access control repository and may considered one embodiment of FIG. 3.

[0018] FIG. 5 is an illustrative embodiment of a software context implemented in the distributed environment of FIG. 3.

[0019] FIG. 6-9 are graphical user interfaces illustrating a browsing session in which a user accesses entitlement services.

[0020] FIG. 10 is an illustrative table maintained with data located in the access control repository.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0021] The present invention provides an access control repository for implementing a common entitlement service. The access control repository is interposed between a front-end environment (i.e., a plurality of clients) and back-end resources containing a plurality of entitlement databases. During a browsing session, clients may invoke a plurality of applications each of which are configured to support different Web based solutions. To determine a customer's entitlement to a particular solution, the applications access a common repository containing entitlement information. Illustratively, the common repository is populated with entitlement information from a plurality of diversified entitlement systems.

[0022] One embodiment of the invention is implemented as a program product for use with a computer system such as, for example, the computer 200 shown in FIG. 2 and described below. The program(s) of the program product defines functions of the embodiments (including the methods described below) and can be contained on a variety of signal-bearing media. Illustrative signal-bearing media include, but are not limited to: (i) information permanently stored on non-writable storage media (*e.g.*, read-only memory devices within a computer such as CD-ROM disks readable by a CD-ROM drive); (ii) alterable information stored on writable storage media (*e.g.*, floppy disks within a diskette drive or hard-disk drive); or (iii) information conveyed to a computer by a communications medium, such as through a computer or telephone network, including wireless communications. The latter embodiment specifically includes information downloaded from the Internet and other networks. Such signal-bearing media, when carrying computer-readable

instructions that direct the functions of the present invention, represent embodiments of the present invention.

[0023] In general, the routines executed to implement the embodiments of the invention, may be part of an operating system or a specific application, component, program, module, object, or sequence of instructions. The computer program of the present invention typically is comprised of a multitude of instructions that will be translated by the native computer into a machine-readable format and hence executable instructions. Also, programs are comprised of variables and data structures that either reside locally to the program or are found in memory or on storage devices. In addition, various programs described hereinafter may be identified based upon the application for which they are implemented in a specific embodiment of the invention. However, it should be appreciated that any particular program nomenclature that follows is used merely for convenience, and thus the invention should not be limited to use solely in any specific application identified and/or implied by such nomenclature.

[0024] FIG. 2 depicts a computer 200 in which embodiments of the invention may be implemented. The computer may be representative of computers used to execute software necessary to implement the software environment shown in FIG. 3, described below. FIG. 2 is merely one configuration for a computer. Embodiments of the present invention can apply to any comparable hardware configuration, regardless of whether the computer system is a client, a server, a complicated, multi-user computing apparatus, a single-user workstation, or network appliance that does not have non-volatile storage of its own.

[0025] In general, the computer 200 includes a Central Processing Unit (CPU) 228 connected via a bus 230 to a memory 232, storage 234, input device 236, output device 238 and a network interface device 237. The input device 236 can be any device to give input to the computer 200. For example, a keyboard, keypad, light-pen, touch-screen, track-ball, or speech recognition unit, audio/video player, and the like could be used. The output device 238 is preferably any conventional display screen and, although shown separately from the input device 236, the output

device 238 and input device 236 could be combined. For example, a display screen with an integrated touch-screen, and a display with an integrated keyboard, or a speech recognition unit combined with a text speech converter could be used.

[0026] The network interface device 237 may be any entry/exit device configured to allow network communications between the computer 200 and other networked devices via the network (shown in FIG. 1), for example. For example, the network interface device 237 may be a network adapter or other network interface card (NIC).

[0027] Memory 232 is preferably random access memory sufficiently large to hold the necessary programming and data structures of the embodiments of the invention. While memory 232 is shown as a single entity, it should be understood that memory 232 may in fact comprise a plurality of modules, and that memory 232 may exist at multiple levels, from high speed registers and caches to lower speed but larger DRAM chips.

[0028] Storage 234 is preferably a Direct Access Storage Device (DASD), although it is shown as a single unit, it could be a combination of fixed and/or removable storage devices, such as fixed disc drives, floppy disc drives, tape drives, removable memory cards, or optical storage. Memory 232 and storage 234 could be part of one virtual address space spanning multiple primary and secondary storage devices.

[0029] FIG. 3 is a distributed environment 300 configured with an access control repository. Some or all of the devices of the distributed environment 300 may be computers such as the one described above with reference to FIG. 2. In general, the distributed environment 300 shows a front-end tier, back-end tier and an intermediate tier. The front-end is defined by a plurality of client computers 302_1, $302_2 \ldots 302_N$ (collectively referred to herein as clients 302) operated by users desiring to access entitlement services data. In a Web-based environment each of the clients 302 execute a browser application 304_1, $304_2 \ldots 304_N$ (collectively referred to herein as browsers 304). Illustrative browsers including Netscape's Navigator® and Microsoft's Internet Explorer®. Although aspects of the invention are described in

the context of a Web environment, the invention contemplates any distributed environment. Accordingly, the particular client application used by the clients 302 will depend upon the resources being accessed.

[0030] The browsers 304 are configured to access the intermediate tier via a network 306. The network 306 may be any Local Area Network (LAN), Wide Area Network (WAN) or combination thereof. In a particular embodiment, the network 306 is the Internet. In one embodiment, information flow between the network 306 and the intermediate tier is restricted by a security mechanism 308. The security mechanism 308 may be, for example, a firewall which may be implemented as software, hardware or both.

[0031] Illustratively, the intermediate tier comprises an Access Control Repository (ACR) 310. The term Access Control Repository (ACR), like all terms used herein, is merely used for convenience and is not intended to restrict the scope of the invention to a particular implementation. The ACR 310 is generally any repository containing entitlement services data. The entitlement services data contained in the ACR 310 is not specific to any particular application or interface, but rather includes (at least in one embodiment) records representing all the entitlements for a given customer of a given enterprise (e.g., corporation). The source of the entitlement services data is the back-end resources 312. Thus, the ACR 310 is populated with entitlement services data from the back-end resources 312, which generally comprises a plurality of databases each containing different entitlement services data.

[0032] It should be noted that the ACR 310 and the back-end resources 312 may be, but need not be, part of a common enterprise. For example, the ACR 310 and the back-end resources 312 may both be maintained by International Business Machines, Inc. Alternatively, the ACR 310 and the back-end resources 312 may be separately maintained. For example, the back-end resources 312 may be maintained by International Business Machines, Inc., while the ACR 310 may be maintained by an independent third party. In the latter embodiment, the ACR 310

may contain entitlement services data for a plurality of enterprises. In this way, customers can enjoy a single access point to all their entitlement services data.

[0033] Referring now to FIG. 4, a distributed environment 400 is shown which may be considered a detailed embodiment of the distributed environment 300 shown in FIG. 3. As such, like numerals denote like components described above. For simplicity, only a single client computer 302 is shown. A navigation page/portal 402 provides an entry point to a plurality of entitlement services (as well as other services) offered by an enterprise. Access to the entitlement services is supported by a Web service 404 which, illustratively, supports any of a variety of communication protocols including XML, HTTP and SOAP. Each of the entitlement services is supported by one or more applications 410. Each application 410 is configured with an Application Program Interface which allows the respective application 410 to make requests for data contained in an ACR database 412 of the ACR 310. In order to handle requests from the applications 410, the ACR 310 is configured with an ACR application server 414 which, in response to a request, accesses the ACR database 412 and returns the appropriate information. In one embodiment, the ACR application server 414 is a Websphere server and the ACR database 412 is a DB2 database, both of which are products available from International Business Machines, Inc.

[0034] The ACR database 412 is populated with information from a plurality of entitlement databases 416. Illustrative records contained in the ACR database 412 will be described below. Connectivity between the ACR database 412 and the entitlement databases 416 is facilitated via one or more adapters 418.

[0035] The processing implemented by the distributed environments 300, 400 is further described with reference to the data processing environment 500 of FIG. 5. In addition, reference is made to FIGS. 6-10 which show examples of user interfaces encountered during a browser session. Again, like numerals identify components introduced above. During a browser session, a user accesses information about their entitlement services by first accessing the navigation portal 402 via a browser 304. An example of a navigation portal is illustrated by the graphical user interface

(GUI) 600 in FIGS. 6. The GUI 600 provides a country field 602 (implemented as a drop-down menu) in which a user may designate a country. The GUI 600 also provides a plurality of hyperlinks, each of which allow the user to access different services. For purposes of illustration, it is assumed that the user clicks on the "Premium services" link 604. As a result, the browser 304 navigates to a premium services page illustrated by the GUI 700 in FIG. 7. Here, it is assumed that the user clicks on a "Web delivered premium services" link 702 causing the browser 304 to navigate to the premium services page illustrated by the GUI 800 in FIG. 8. The GUI 800 provides a plurality of links 802 for different products having Web based services. Each of the links 802 may be associated with one of the applications 410. As a result, the user invokes an application 410 by clicking on any of the application's respective links. By way of illustration, it is assumed that the user clicks on a first link 804 which provides services for the iSeries and AS/400 computers. Clicking on the first link 804 causes the browser 304 to navigate to the GUI 900 shown in FIG. 9. The GUI 900 provides a sign-in interface comprising a user ID field 902 and a password field 904. Successfully signing in requires the user to first have registered. Once registered, the user can enter the appropriate information into each of the fields 902, 904 and access the services for the designated products. In particular, the user may invoke the appropriate application 410 to access entitlement services data contained in the ACR database 412.

[0036] Referring back to FIG. 5, retrieval of entitlement services data contained in the ACR database 412 is initiated when the user issues a request (e.g., by clicking on a link or submitting sign-in information) from the browser 304 via the network 306. An application 410 invoked by the request then issues a query 505 to the ACR application server 414 to determine whether the user is entitled. A response to the query is generated by the application server 414 by accessing the database 412 to determine whether any records exist for the request to user. Any relevant records are then return to the requesting application 410.

[0037] In this manner, each request for entitlement services data is handled by the ACR 310 regardless of the application 410 being invoked. In addition, each of the applications 410 may share data between one another. At one level, data

sharing occurs because the applications 410 have access to a common repository: the ACR database 412. However, in a particular embodiment, the applications directly pass entitlement services information between one another. For example, when a user accesses a service supported by Application 1, Application 1 operates to retrieve entitlement data for the user from the ACR database 412. When a user then accesses services supported by Application 2, the entitlement data retrieved by Application 1 is passed to Application 2. Accordingly, Application 2 need not issue a request to the ACR server 414, which is a relatively expensive operation. In this manner, one aspect of the invention achieves greater performance than is available with prior art entitlement systems.

[0038] In another aspect, consolidation of entitlement services data allows an enterprise to offer services not possible with prior art entitlement systems. For example, as described above, where the entitlement services data is distributed over a plurality of databases, no feasible solution for extending complementary services to customers of an enterprise. Embodiments of the present invention overcome the limitations of the prior art by consolidating the entitlement services data into a common repository. Each application, regardless of the specific services which it supports, now has access to all services to which a customer is entitled.

[0039] As noted above, the ACR database 412 is populated with information from the entitlement services databases 416. In one embodiment, the population of the database 412 is managed by the adapters 418. Population of the database 412 may be performed, for example, when a user enters through the navigation page 402 and registers a product through a particular application 410. The application interface then notifies the appropriate adapter 418 to replicate data contained in the entitlement services databases 416 to the ACR database 412.

[0040] Referring now to FIG. 10, an illustrative ACR table 1000 is shown. The table 1000 is representative of a table contained in the ACR database 412. In general, the table 1000 is formatted as a plurality of columns and rows, were each row defines a record. Illustratively, the table 1000 includes a user ID column 1002, an asset ID 1004, a service ID 1006, a subservice ID 1008, a country code 1014,

and an application ID 1012. The user ID may be any combination of alphanumeric characters which a user provides at the time of registration. The asset ID uniquely identifies the particular product to which entitlement services attached. The service ID and subservice ID represent the services to which the user is entitled (e.g., problem management, performance management, etc.) as defined by the applications 410. The country code specifies a country specific to the product and entitlement services. The application ID specifies participating applications for authentication of the applications. In this manner, the application ID prevents unauthorized applications (e.g., such as an application created by a hacker) from accessing the database 412. For a given user, a separate record exists for each combination of assets, services, country and application.

[0041] It should be understood that the table 1000 is merely illustrative. Persons skilled in the art will recognize that the table 1000 may be formatted to contain additional (or in some cases less) information.

[0042] While the foregoing is directed to embodiments of the present invention, other and further embodiments of the invention may be devised without departing from the basic scope thereof, and the scope thereof is determined by the claims that follow.